Blockchain-based Mobility-as-a-Service

Tri Hong Nguyen
University of Oulu
Oulu, Finland
tri.nguyen@oulu.fi

Juha Partala
University of Oulu
Oulu, Finland
juha.partala@oulu.fi

Susanna Pirttikangas
University of Oulu
Oulu, Finland
susanna.pirttikangas@oulu.fi

***Abstract*—In this paper, we present a vision for a blockchain-based Mobility-as-a-Service (MaaS) as an application of edge computing. In current MaaS systems, a central MaaS operator plays a crucial role serving an intermediate layer which manages and controls the connections between transportation providers and passengers with several other features. Since the willingness of public and private transportation providers to connect to this layer is essential in the current realization of MaaS, in our vision, to eliminate this layer, a novel blockchain-based MaaS is proposed. The solution also improves trust and transparency for all stakeholders as well as eliminates the need to make commercial agreements with separate MaaS agents. From a technical perspective, the power of computing and resources are distributed to different transportation providers at the edge of the network providing trust in a decentralised way. The blockchain-based MaaS has the potential to emerge as the main component for a smart city transportation offering efficiency and reducing carbon dioxide emissions.**

***Index Terms*—Mobility-as-a-Service, MaaS, blockchain, blockchain-based MaaS, smart contract, intelligent transport systems, edge of things, security.**

I. Introduction

Transportation is one of the most critical components of the global economy. As the volume and speed of transportation in moving goods and people have grown significantly in the recent years, it is essential to also improve the capacity and efficiency of transport e.g. through the means of digitalisation. Intelligent Transport Systems (ITS) have a significant role in trading and exchanging products and people which also impulses growing economy. We examine the Mobility-as-a-Service (MaaS) as an effective candidate for transport systems in the future.

Obviously, a journey planner or trip planner is one of the most important features of a smart transportation system. It is witnessed as a search engine to recommend several possible routes from a source to a destination based on integrating different means of transport from a large number of sub-routes [1], [2]. In addition, for a travel service platform, the payment methods should offer the travelers' preferred strategies. For example, choosing "pay-as-you-go" or "mobility package" (for the monthly or annual package) should be valid options. For ticketing, current smart cards, e-tickets or hard-copies (traditional ticket) are used. These kinds of ticket have recently utilized either Near-Field Communication (NFC) or Barcode as state-of-the-art technologies. However, to set up the same technology for ticket validation between different providers is not an easy task since each provider has had its own scheme. In the term of managing the services, that is, providing verified and confirmed tickets between travelers and providers, an approach which can manage and validate tickets from different providers who are a part of the selected route is required.

With these issues to form a transport platform, MaaS is considered as the perfect solution which includes a trip planner, e-ticket, payment method (both "pay-as-you-go" and "mobility package") and also validated ticket scheme. The current MaaS systems, in particular, have been implemented as a centralized intermediate layer between providers and travelers. With this idea, MaaS system has several advantages such as the easy management of two-sided (travelers and providers) and a common database of different providers; however, it also will be a huge challenge if the MaaS network or the model desires to scale up with many different providers.

Edge computing brings computation and the required storage near the location where they are needed. Services and computing power are shifted from centralised nodes to distributed nodes closer to the users reducing latency and transmission costs. With the use of edge computing, MaaS services naturally benefit from localisation. For example, travel within a single city could be conveniently implemented under a monthly subscription model. However, shifting from a traditional centralized MaaS to distributed computing requires a new approach.

Due to the development of blockchain technology and especially the idea of the smart contracts, we expect that a new distributed approach to MaaS systems can be achieved. In addition, blockchain technology will improve transparency and trust between providers by eliminating the intermediate layer. Instead, blockchain technology with smart contracts executed on the edge can directly connect travelers to providers in a more efficient manner. Therefore, a blockchain-based MaaS can achieve many advantages including validation, confirmation, and formation through smart contracts. Specifically, the tickets and payment methods particularly can be programmed as smart contracts stored and verified in blockchain by different transportation providers. To make this idea become a reality, a blockchain-based MaaS has to address several

This is the authors' accepted version. The final version is published by IEEE in The 28th International Conference on Computer Communications and Networks (ICCCN 2019) July 29 - August 1, 2019, Valencia, Spain. This work is made available online in accordance with the publishers policies. Please refer to any applicable terms of use of the publisher.

issues from journey planner and blockchain technology when adopting these methodologies.

The remaining of this paper is organized as follows. The next section (section II) illustrates a general background of technologies in blockchain-based MaaS system, while the description of the novel MaaS adopting blockchain technology is showed in section III. Finally, section IV is to summarize the paper.

II. Background and Technologies

A general background of the proposed technologies is described in this section. In the beginning, a description of ITS is provided. After that, the overall ideas of using a journey planner and utilizing blockchain technology are depicted as components of blockchain-based MaaS. Finally, a short evocation of EoT is referred to with blockchain-based MaaS.

A. Intelligent Transport System (ITS)

To start with the idea of ITS, [3] indicated that ITS is an application or system utilizing advanced technologies in the management of transportation in order to improve the efficiency of transport systems. ITS hence has a significant role in trading and exchanging products and people, which impulses growing economy. From a technical point of view, the integration of different transportation modes as a plan of a journey from a source to a destination is a critical part of logistics. Furthermore, low-latency and reliable mobile connections are essential for scalable and trusted transfer of mobility data. From that perspective, we examine MaaS as an effective candidate for the transport systems in the future.

B. Mobility-as-a-Service (MaaS)

MaaS is seen as a unifying platform for different transport services for a personalized journey with a single ticket. MaaS aims to gather the transport sector operators in a co-operative, interconnected ecosystem (involving transportation services, transport information, and payment services) providing services matching the needs and behavior of customers [4]–[6]. The service provides personalized bundles or packages which offer the best option for every journey as a real alternative to owning a car (e.g. a taxi, public transport, a rental car or a bike share) leading to the reduction of carbon dioxide, also [7]–[9]. From these views of MaaS, a collection of main characteristics in MaaS showed by [10] consisting of the integration of transport modes, tariff option, one platform, multiple actors, use of technologies, demand orientation, registration requirement, personalization, and customization. From the business model point of view, one of the main challenges of MaaS is the willingness of public and private transportation providers to interface and work with MaaS agents fronting the customers.

C. Journey Planner or Trip Planner

A key requirement for MaaS systems is a journey planner which is considered as a transportation search engine. In a general description, a journey planner responds any requests for a path from A to B. Due to the difficulty of a single transport mean supporting from A to B, a proposal is about a route integrating with different transport means to become an integrated journey planner [11]. Moreover, with a variety of different paths and demands of travelers, the journey planner systems should also reply as many as possible routes which can connect A and B. For example, the route from A to B can be recommended and arranged based on travelers' demand such as fastest, cheapest and the most comfortable.

D. Blockchain Technology

In a nutshell, blockchain technology is showed and considered as a technology with plenty of advantages in security to build communicative systems with the first introduction and application of cryptocurrency named Bitcoin [12]. Particularly, it is a data structure based on cryptographic algorithms to track, record and verify transactions across the network between participants [13]. Due to sharing a unique data structure between nodes, it aims to form an immutable chain of blocks with tamper-resistant characteristic through hash functions. Therefore, blockchains may be described as databases which are distributed in a decentralized network instead of traditional centralization. With the decentralized network, the third parties in interactive applications are eliminated, which leads to a trusted environment between members of the network. Furthermore, the system can reduce cost and time due to transactions transparently transferred between nodes. After the development of blockchain-based cryptocurrencies, other interactive applications attempt to apply blockchain technology to solve their existing problems. One of the most popular examples is the introduction to Ethereum [14] which contains and transmits plenty of resources such as transactions and operating codes.

E. Edge of Things (EoT)

With the explosion of data at the edge of the network (e.g. from gadgets) [15], there has been raised questions about the efficiency of data processing. Although cloud systems are able to process enormous amounts of data, the bandwidth of the network and privacy issues in connectivity are identified as challenges. Expressly, the swift growth of IoT devices impact on traditional cloud systems such as bandwidth, computing resources, privacy and also energy efficiency.

From this perspective of traditional cloud computing, a new term called edge computing is proposed as an effective solution for these challenges. In a short description from [15], edge computing allows computations or processes at the edge of the network without the requirement to transmit raw data to process at central servers. In other words, to compare with existing works as fog computing, [15] indicated that edge computing pays attention to the things side instead of infrastructure side from fog computing. As a consequence, edge computing is considered as an effective solution for current issues (reliability, security, and privacy) in central systems.

In term of blockchain-based MaaS, without an intermediate layer, the data of transportation providers do not need to

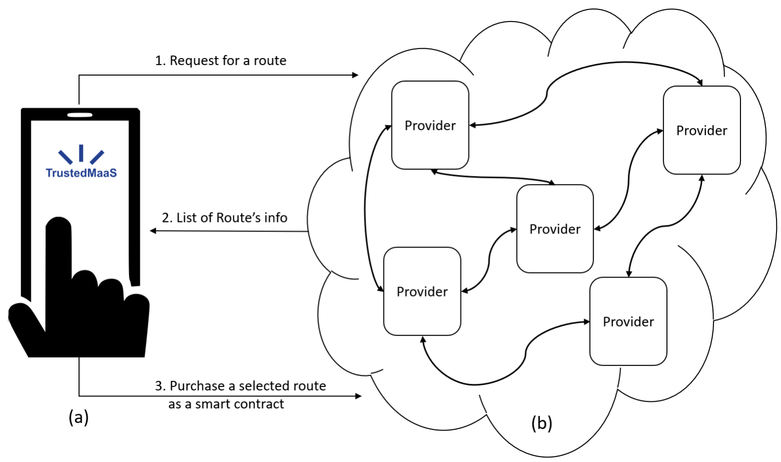

Fig. 1. An overview of blockchain-based MaaS, in the beginning, a traveler (a) sends a request for a route. The set of transportation providers (b) then communicate and propose a list of possible routes' information. After that, the traveler selects and forms their preferred route (based on a set of different transport means) as a smart contract. This smart contract is checked and confirmed by the providers before storing in the next block to extend the blockchain.

transmits to central servers as a cluster. As an alternative, blockchain-based MaaS asks different transportation providers to receive and handle request from travelers through their database of routes. This data can be shared and synchronized between different local providers. Thus, the computation of the network is distributed as the idea of EoT.

III. Blockchain-based MaaS

In this section, we desire to describe blockchain-based MaaS. To start with the vision of blockchain-based MaaS, a description of a suitable consensus mechanism and incentive strategy is discussed. After that, the challenges of blockchain-based MaaS are mentioned through privacy, security, and issues of the journey planner system. Finally, the expectation and impact of blockchain-based MaaS are considered.

A. Vision of Blockchain-based MaaS

With the utilization of blockchain technology, the MaaS system cannot only obtain verified and confirmed scheme through a set of different transportation providers, but it also achieves blockchain's advantages including the transparency of transmitted data and trust between transportation providers without a middle layer of MaaS in the system. In addition, MaaS can utilize existing blockchain-based platforms with a wide range of their features and functions in which MaaS' characteristics can be suitably satisfied such as payment, identification, and the idea of the smart contract. In more detail, with the idea of containing source codes in blockchain as smart contracts, the integration of transport modes can be formed by the travelers as their preferred. Moreover, with the consortium blockchain, the permission for operations in blockchain can be separated, which allows being managed by controllers and sellers of transport means.

In a general view as Fig.1, blockchain-based MaaS consists of two main types of participants including transportation providers playing a role as miners in blockchain-based cryptocurrency systems and travelers or clients who receive routes' information from the providers to form their own route as a smart contract (based on their preferred). Therefore, the blockchain in this system is managed and maintained by those providers (this blockchain has to be in the same as other provider's). In detail as Fig.2, if a traveler requests a route from A to B, he/she will receive a set of the information displaying as many as possible ways from which the traveler can select a possible list of different transport modes. He/she then forms a smart contract before replying it back to the network. Once receiving this smart contract, providers in blockchain-based MaaS attempt to verify and confirm prior to putting on the current block. To verify the smart contract from the traveler, the providers have to check the information of transport modes in the smart contract with their data of routes. If these transport modes are correct and satisfied requirements, this smart contract is added into the current block which waits to append and extend the blockchain. Accordingly, the transportation providers in the system have to share its routes to other providers to verify smart contracts and enhance the probability of its route suggested to travelers. In addition, to avoid wrong routes which are generated by providers' bad behavior, there is an idea of using a voting system in which each transportation provider has to verify submitted smart contracts based on their knowledge from data of routes before sending an agreement of this smart contract to neighbors. Particularly, if there are more than a threshold θ (a number of agreements on a smart contract from providers in the network), this smart contract can be satisfied and then added to the current block. Due to the voting system, the transportation providers in the system have to share their knowledge of routes in order to obtain the agreement from other providers.

One of the principal questions to build applications based on blockchain technology is the consensus mechanism which runs a mean of the connection and distribution of data or blocks to form a unique set of data or blockchain across the asynchronous network. Without exception, we hence need

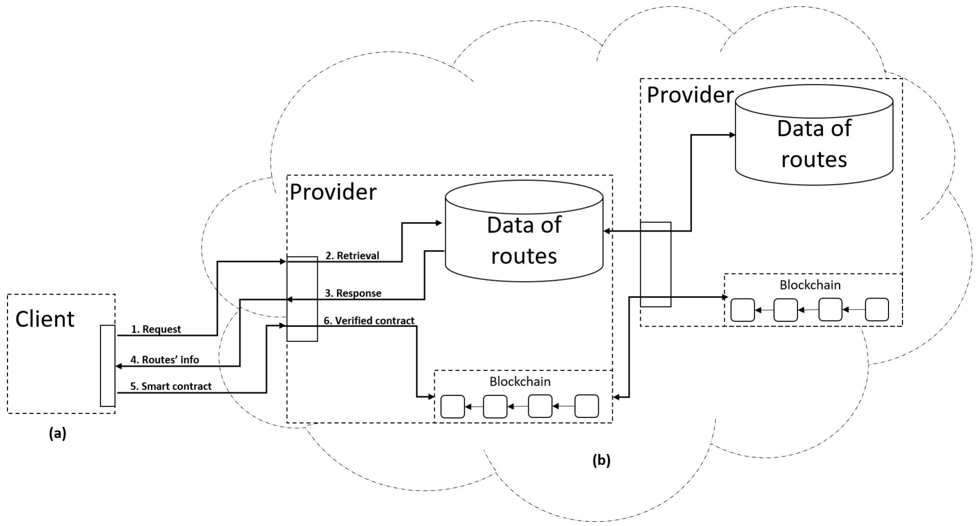

Fig. 2. The specific communication between a traveler and a transportation provider with (a): client-side and (b): server-side (a set of different transportation providers).

to consider a suitable consensus mechanism for blockchain-based MaaS. In particular, after collecting enough verified smart contracts, there are several approaches to close the current block (stop collecting more verified smart contracts added in the current block) such as solving a specific task, waiting for a period of time or obtaining a fixed number of verified smart contracts. Once closing the current blocks, transportation providers can generate their block as a candidate to extend the blockchain. Due to an asynchronous network, each transportation provider can receive and verify different smart contracts before forming a block which can be different from other transportation providers' block. As a consequence, after closing the current block, each transportation provider broadcasts its block to neighbors. If a transportation provider receives greater than a threshold δ the same block, it will append this block to the blockchain.

Another idea going along with current consensus algorithms is the incentive strategy introduced by Bitcoin [12] to prevent fault miners. In the case of blockchain-based MaaS, we also consider it as a way to encourage providers to participate in the voting process. After a purchase of a selected route, the travelers need to pay for an extra fee which rewards providers for participating the voting process of the selected route. Moreover, the amount of extra fee depends on the period between the purchased and departure date. If the purchased date is close to the departure date, as an example, the cost will be more expensive than a wide period between the purchased and departure date due to the requirement for fast confirmation as the level of priority. Furthermore, this strategy can be considered as an approach to encourage providers to share routes' information to travelers despite competitive providers' information.

Since traditional MaaS systems collect entire routes' information and verify tickets through a cluster of servers, it will raise a situation about the scalability of networks. MaaS can obtain several advantages from blockchain's benefits. The key merit for adopting blockchain in the MaaS system is the elimination of the intermediate layer between the providers and travelers. Therefore, the routes' information is not needed to transmit to centralized servers. Instead, transportation providers exchange their data among them. With this point of view, a proposal can be considered through the use of edge computing that each smart city will have a specific blockchain containing smart contracts of statuses of the movements (e.g starting, finishing and paying the trips) in that city. Moreover, this blockchain is maintained by transportation providers of that city. As one big problem with blockchain is the requirements of heavy computation due to the explosion of blockchain with a large amount of essential information, here, the city's blockchain is managed by local transportation providers who serve the transportation for the city. Similarly, in the case of a country, another blockchain can be used to store movements between cities of the country; meanwhile, to connect between nations, it requires a different blockchain which contains valid international transport routes. With this idea based on the hierarchy of blockchains, new transportation providers can consider and join in blockchains related to regions that they would like to contribute without requirements storing a huge blockchain and data of routes. As the boundaries of cities is also a vague concept, we could start dividing these regions into areas based on other metrics, like the density of transportation services. Nevertheless, this proposal can raise several other issues about the connection between different blockchains and between datasets of routes for verification and confirmation on smart contracts such as a novel consensus for inter-blockchains being similar to a hybrid blockchain architecture for IoT [16] and the necessary routes' information which should be transferred between different blockchains.

As a way to decentralize data including blockchains and routes' information, the idea of edge computing can be considered as an efficient architecture supporting blockchain-based MaaS' providers to control the flow of data as the idea from the hierarchy of blockchains above. Particularly, it can be seen from Fig. 2 that the proposal blockchain-based MaaS requires a protocol collecting, propagating and recommending routes' information on two sides (provider-provider and provider-traveler). Meanwhile, another protocol needs to deliberate between different providers for verification of smart contracts and decisions of consensus mechanism. Thus, an utilization of edge computing cannot only become a fit and efficient architecture for these communicative protocols, but it also supports for optimization of powerful computations in issues related to journey planner and consensus mechanism. Particularly, it can reduce the cost of redundant computation and transmission on journey planners' or other relevant transport data. Therefore, the routes' information and messages of the consensus mechanism in each city (or region) do not need to transmit to other transportation providers outside the selected boundaries (or region). From that perspective, transportation providers can use edge servers to store and process real-time information for mobile clients, which satisfies the demands in the swiftest way. For example, if there is a delay with a mean of transportation in a city, the journey planner can recommend a better replacement using local, up-to-date resources. To immediately resolve this matter, the use of edge servers or journey planners in this specific place play a crucial role for re-routing and re-verifying the trip again.

B. Challenges and Opportunities

With the view eliminating the intermediate layer, a blockchain-based MaaS system has to adopt and deal with several issues from blockchain technology, smart contract, and journey planner system. Thus, this subsection mentions challenges and problems which have to be considered in the construction of a blockchain-based MaaS.

1) Confidentiality in Blockchain: One of the main issues that need to be addressed is user privacy. Smart contracts need to be automatically enforced in the blockchain network. Typically, this means that the contracts need to specify the contractual terms and statements in the clear. However, these statements include personal information related to passengers. Cryptographic *zero-knowledge argument schemes* (SNARKs) can be applied to demonstrate that the terms have been satisfied without disclosing private information in the contract. These methods are vital in the secure implementation of our vision.

Due to a public network in which participants can join and leave freely, the privacy of users is the most crucial part needing to be noted by the system. There are many reasons which a MaaS requires users' information as previous analyses of MaaS. Generally, a MaaS system desires to utilize travelers' history (previously selected routes) to indicate fit routes and also reward travelers for their loyalty such as vouchers. However, if this information is put into a public or consortium blockchain, there will be plenty of problems. Wrongdoers, for example, can witness and keep track of travelers' private schedule or even exactly know current location of travelers. In financial blockchain applications, transaction details can be hidden with a zero-knowledge argument scheme, which has been already demonstrated by cryptocurrency Zcash [17]. It utilizes SNARKs to guarantee the validation on transactions in the network without vision on information of senders, receivers and transaction values. This is seen as a promising approach to enhance the privacy of existing blockchain technology. Another example being Ethereum has applied this approach in its development [18].

2) Security of Smart Contracts: Another issue to form a MaaS based on the smart contract with blockchain technology is the adoption of both its benefits and issues. As a survey of vulnerabilities on smart contracts with Ethereum as a case study, [19] divided existing smart contract's attacks into three main groups (programming language - Solidity, Etherum Virtual Machine - EVM, and blockchain). Additionally, they mentioned the difficulty to recognize security problems or mistakes from programmers when those can propose contracts from their side. In particular, as most security mistakes come from programmers, these problems cannot be completely prevented but they can be mitigated as long as the programmers are trained with practical experience or even provided tools based on static analysis researches to support low-level analyses. From this perspective, a strict default form on smart contracts for blockchain-based MaaS system can be considered to limit programming mistakes. Additionally, it requires research to utilize static analysis approaches in order to decline the number of security mistakes from smart contract builders.

3) Issues of Journey Planner: In term of journey planner, a blockchain-based MaaS also has to face issues related to a common format in order to share and combine data from different transportation providers. It is clear that to form a whole route with a set of different transport means, the system can require a default format on data for different providers and also a suitable algorithm for retrieval of routes in the database. Meanwhile, in term of traditional MaaS schemes, they have run as a middle layer to support this challenge of journey planner. In blockchain-based MaaS, it hence requires a standard format for the system and the providers have to convert to this data format before sharing to construct a data set of routes.

Another issue with a journey planner is about the constant modification of routes' information such as the price and the departure time. In particular, current journey planners are based on graph algorithms in order to seek suitable routes. Those thus consider to construct a graph and load it to the main memory or cache for fast retrievals, calculations, and responses. However, if there are several changes after building the graph, it will be hard to jump to memory to modify the information. This issue can become one of the main problems in an asynchronous system as blockchain-based MaaS. Moreover, if there are a large number of providers who join and leave constantly the system, the graph has to rebuild and then impact on provider's resource. With these situations, heuristic solutions can be considered with the use of edger computing. For example, the graph can be reconstructed after the blockchain is extended with a new block or a fixed period of time.

C. Expectations

Blockchain-based MaaS is anticipated at the outset of distributed MaaS systems with the utilization of blockchain technology because of its advantages such as trust between providers, flexibility (new providers can freely participate the network) and also the transparency (between providers and travelers) in the decentralized network. In addition, it forms a novel MaaS as smart transportation playing a notable part in smart cities. From the viewpoint of the methodology, at the beginning of blockchain-based MaaS, a study on a fit consensus algorithm for blockchain-based MaaS is one of the first considerations due to its prime role in a blockchain-based system. Meanwhile, blockchain-based MaaS also requires a study of recent journey planner platforms. After that, it requires concentrating on privacy and the security of the system as mentioned above. Particularly, the use of zero-knowledge arguments is essential for ensuring privacy, whereas the application of static analysis is required to argue and analyze the security of smart contracts.

D. Impact

With the high demand for transportation, MaaS is considered one of the fit solutions for future smart transportation strategy. However, with the current centralized MaaS background architectures, the systems lack flexibility, trust, and transparency and make national and cross-border MaaS difficult to realize. To be able to create governance, where anyone can connect to any service providers with a trusted connection, would lead to a digital open market. With blockchain technology, the need for separate MaaS operators would be obsolete and the service providers could connect their services for full journeys in a peer-to-peer manner. Here, the need for extra commercial agreements between service providers and MaaS operators vanishes, also. However, mutual governance, sharing of data, plans, and timetables are necessary. In Finland, *The Transport Code* makes this possible, as it mandates all transportation providers to open data and APIs to third parties (law effective from Jan 2018). Furthermore, access to the users' behavioral data would lead to a means to develop the whole ITS with artificial intelligence.

IV. Conclusion

With the idea of adopting blockchain technology, the intermediate layer of MaaS systems is eliminated to form a new term called blockchain-based MaaS. Blockchain-based MaaS is considered an effective solution to building a smart transport platform as a decentralized network in which the transportation providers can verify and confirm their tickets through a blockchain containing smart contracts as tickets. Due to this network formed by transportation providers, it is expected as a transparent and trusted network where different transportation providers can flexibly participate. Therefore, it can become an open market for transportation providers. However, to construct the blockchain between transportation providers, the network requires a suitable consensus mechanism to form a unique blockchain and a communicative protocol for the shared database of routes. Additionally, once adopting blockchain technology, the network needs to considered existing blockchain's issues including privacy and security problems. In term of scalability problem, the edge computing can provide a fit architecture to support the hierarchy of blockchains and swift processes of real-time routes' information for travelers at the local.

Acknowledgment

This research is done in a strategic research project *Personalization, Privacy and Quality Control for MaaS with Blockchain - TrustedMaaS* under focus institute Infotech Oulu, University of Oulu. Furthermore, the researchers operate under Academy of Finland 6Genesis Flagship (grant 318927).

References

[1] J.-Q. Li, K. Zhou, L. Zhang, and W.-B. Zhang, "A multimodal trip planning system with real-time traffic and transit information," *Journal of Intelligent Transportation Systems*, vol. 16, no. 2, pp. 60–69, 2012.

[2] K. Zografos, V. Spitadakis, and K. Androutsopoulos, "Integrated passenger information system for multimodal trip planning," *Transportation Research Record*, vol. 2072, no. 1, pp. 20–29, 2008.

[3] E. P. (EP), "Directive 2010/40/eu of the european parliament and of the council of 7 july 2010 on the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other modes of transport," 2010.

[4] S. Hietanen, "Mobility as a Service," *The New Transport Model*, pp. 2–4, 2014.

[5] P. Holmberg, M. Collado, S. Sarasini, and M. Williander, "Mobility as a service-maas: describing the framework: final report maas framework," 2016.

[6] J. Sherly and D. Somasundareswari, "Internet of things based smart transportation systems," *International Research Journal of Engineering and Technology*, vol. 2, no. 7, pp. 1207–1210, 2015.

[7] F. Nemanu, J. Schlingensiepen, D. Buretea, and V. Iordache, "Mobility as a Service in smart cities," *Responsible Entrepreneurship Vision, Development and Ethics*, p. 425, 2016.

[8] E. Gould, W. Wehrmeyer, and M. Leach, "Transition pathways of e-mobility services," *WIT Transactions on Ecology and the Environment*, vol. 194, pp. 349–359, 2015.

[9] D. König, J. Eckhardt, A. Aapaoja, J. Sochor, and M. Karlsson, "Business and operator models for Mobility as a Service (MaaS) (deliverable 3 to the MAASiFiE project)," *Brussels: Belgium*, 2016.

[10] P. Jittrapirom, V. Caiati, A.-M. Feneri, S. Ebrahimigharehbaghi, M. J. Alonso González, and J. Narayan, "Mobility as a service: A critical review of definitions, assessments of schemes, and key challenges," 2017.

[11] M. Rafiah, J. R. Rice, J. S. G. Ferguson, A. J. Sadler, and P. R. Harrison, "Integrated journey planner," Dec. 21 2004. US Patent 6,834,229.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[13] H. Natarajan, S. Krause, and H. Gradstein, "Distributed ledger technology and blockchain," 2017.

[14] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[15] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[16] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains," *arXiv preprint arXiv:1804.03903*, 2018.

[17] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy (SP)*, pp. 459–474, IEEE, 2014.
[18] T. Koens, C. Ramaekers, and C. van Wijk, "Efficient zero-knowledge range proofs in ethereum," 2017.
[19] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *Principles of Security and Trust*, pp. 164–186, Springer, 2017.